

**NAVSUP Guide
to System
Certification & Accreditation**

September 1999

PURPOSE: The purpose of this guide is to provide information to the NAVSUP Information System Security Managers (ISSMs) to assist in system accreditation.

REQUIREMENT: CNO mandated message, R 081949Z SEP 99 PROTECTING UNCLAS NETWORKS FROM EXTERNAL THREATS, promulgates a baseline set of security requirements for all UNCLAS Wide Area Network Connections. All information systems and networks shall be certified and accredited as soon as possible, but no later than 15 Dec 99. Every site System Security Authorization Agreement (SSAA) must identify the security mechanisms, configurations, CONOPS, and policies applicable to each wide area network connection and acknowledge the residual risks being assumed by the Designated Approval Authority (DAA) upon Accreditation.

INTRODUCTION: *Certification* is the comprehensive, fully documented, evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process. When this documented level of protection and/or risk is considered to be acceptable by the DAA the system accreditation can take place. *Accreditation* is the formal authorization by an accrediting official, i.e. DAA, for system operation and a clear acceptance of risk. It is a form of quality control on which critical decisions are made regarding the adequacy of security safeguards. A decision based on reliable information about the effectiveness of technical and non-technical safeguards and the remaining risk is more likely to be a sound decision. Achieving Accreditation is a labor-intensive effort. This guide provides a high-level process for assisting you in achieving baseline accreditation within the NAVSUP claimancy.

To be able to achieve a quality accreditation by specific time limits, you should think of what is most critical in today's environment, i.e. are all patches loaded, is the Operating System configured securely according to the guides available, are only allowed protocols being passed through the firewall, etc. Ensure these critical items are considered, tested, and certified before trying to perform a lengthy, in-depth certification and accreditation when trying to meet a fast approaching deadline. Once you have accredited the critical specifics, then make certain you go back and perform a more detailed process to include all specifics.

Before beginning the process of accrediting systems, you must identify key role players, i.e. the Designated Activity Authority (DAA), the Program Manager (PM) of the specific system, Certification Authority (CA), security teams, and user representatives. The DAA is usually an activity's Commanding Officer with the authority and ability to evaluate the system operations in view of the security risks. (In some cases, the

DAA may designate the CA to act in his/her behalf). The PM represents the interests of the system acquisition or maintenance organization with responsibility for daily operations, performance, and maintenance. The CA and security teams are the technical experts that support the C&A process. User representatives ensure the requirements of their needs and expectations are met.

To achieve certification and accreditation there must be in place a documented Security Plan, Risk Assessment (Vulnerability Assessment), Security Tests and Evaluations (ST&Es), and a Contingency Plan. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)" establishes and defines a process that standardizes all activities leading to a successful accreditation. The System Security Authorization Agreement (SSAA) is the agreement that documents all the results of the Certification and Accreditation process.

For SSAA samples see:

URL <http://www.navsup.navy.mil/pki/index.html> Click on [SBU Information](#) button on left-hand side. Click on [Certification and Accreditation Documentation](#). See [System Security Authorization Agreements](#). Samples include DISA tools and templates, generic templates, and a Fleet SSAA. See also [Optional Documentation for SSAA](#) for sample documents, which can be/are, included in a SSAA.

PROCESS: Following are the steps necessary to complete in order to achieve accreditation. For each step, there are templates available to assist you in accomplishing the requirement. Remember that they are only templates and requirements are always different per system/site. Keep this in mind as you develop each document. These templates are available for access/download on the NAVSUP INFOSEC SBU server. For each step, a URL(s) is given for easy accessibility.

When certifying and accrediting your systems, the following priority of systems to be accredited is suggested for the NAVSUP claimancy:

- Network Connections (i.e., NIPRNET, INTERNET)
- Note: SMARTLINK will be addressed at the program level
- Web Servers
 - Firewalls
 - Routers
 - Network Servers
 - Networks
 - Workstations/Laptops

1. Security Plan: Serves as the central tool for establishing an INFOSEC program and assigning responsibilities for the program

implementation and management. It is an essential document in the accreditation process.

For Security Plans samples see:

URL <http://www.navsup.navy.mil/pki/index.html> Click on **SBU Information** button on left-hand side. Click on **Certification and Accreditation Documentation**. See **Security Plans**. Samples include DISA preparation guides, generic ISSP template, and a San Diego-developed ISSP.

2. Risk Assessment: This is the process of analyzing IT threats and vulnerabilities to determine the risk if the system is operated. The Risk Analysis is then used to identify appropriate cost-effective countermeasures to lessen the risk. There are basically two concepts to be defined in this step:

a. Development Certification (CT&E)

This is the technical security assessment of the "as built" system. This is a statement validating the adequacy and effectiveness of security features designed into the system by the developer. It describes the security properties designed into the system and validates their effectiveness.

b. Operational Site Certification (ST&E)

This is the security assessment of the "as fielded" installed system, i.e. site implementation, at the operational site. This statement assesses the residual risk, i.e. the security services met through local physical, administrative, procedural, etc. methods, to ensure protection of the system and the information.

The CT&E identifies the security features provided in a product and upon implementing site-specific security measures to complement those inherent features in protecting the system and its information, the ST&E fully describes these local security measures.

Certification Tests & Evaluations (C, T & Es) and Security Tests & Evaluations (S, T & Es) and their documentation verify and provide evidence that a requirement(s) has passed or failed according to an established criterion. This documentation, i.e. a test report or technical report, is provided to a certification authority (CA) who assesses the results, makes conclusions and recommendations based on these results and provides a certification statement to the accreditation authority who then makes an accreditation decision based on this statement. This procedure ultimately produces the required evidence that ensures the system operates in a secure manner with an acceptable level of risk

For Risk Assessment samples see:

URL <http://www.navsup.navy.mil/pki/index.html> Click on [SBU Information](#) button on left-hand side. Click on [Certification and Accreditation Documentation](#). See [Risk Assessments](#). Samples include a DISA preparation guide and a San Diego-developed report and survey.

For ST&E and Checklist samples see:

URL <http://www.navsup.navy.mil/pki/index.html> Click on [SBU Information](#) button on left-hand side. Click on [Certification and Accreditation Documentation](#). See [Security Tests and Evaluations](#) and [Checklist](#). Samples include generic plans, DISA preparation guides, a FISC San Diego-developed ST&E, DISA checklists, and a FLEET checklist.

3. Contingency Plan: The purpose of a contingency plan is to lessen the damaging consequences of unexpected and undesirable events of whatever size. The probability of an occurrence of an undesirable event is generally inversely related to its size. The greater the catastrophe, the lower the probability it will happen. System operations are disrupted with far greater frequency by small problems than by large ones. Plus, the size or scope of a catastrophe and its effect on system operations are often not directly related. If you do not have a good plan, minor damage can cause major problems. On the other hand, with a good plan even major damage may not result in serious losses.

For a Contingency Plan sample see:

URL <http://www.navsup.navy.mil/pki/index.html> Click on [SBU Information](#) button on left-hand side. Click on [Certification and Accreditation Documentation](#). See [Contingency Plans](#). The sample is a generic plan.

4. Accreditation Decision: The culmination of steps 1 through 3 above results in the preparation of an accreditation package and a recommendation from the Certification Authority for the DAA to approve/disapprove the system to begin operation.

For Accreditation Reports/Letters samples see:

URL <http://www.navsup.navy.mil/pki/index.html> Click on [SBU Information](#) button on left-hand side. Click on [Certification and Accreditation Documentation](#). See [Accreditation Reports/Letters](#). Included is a San Diego report and sample letters.

5. Maintenance: Accreditation maintenance is necessary to ensure secure system management, operation and maintenance to preserve an acceptable level of risk. It begins as soon as the system has been put into operation and accredited and continues until the information system is removed from service, a major change is planned for the system, or a periodic compliance

validation is required. An accreditation statement is good for three consecutive years from the date on the accreditation letter. The accreditation statement is a living document. NAVSUP recommends a bi-yearly review.